CORR 2000-36

On Modular Reduction

Huapeng Wu

Abstract In this paper, an algorithm to partially evaluate modular reduction without division is proposed. A proof of the correctness of the algorithm is given. For a family of generalized Mersenne numbers $N = 2^n - 2^m - 1$, $0 < m < \frac{n+1}{2}$, we show that the modular reduction operation $A \mod N$, where $A < N^2$, can be reduced to

$$A \mod N \equiv A_1 + A_2 + A_4 + 2^m (A_3 + A_4),$$

where $A_1 \equiv A_1 + A_2 \times 2^n$, $0 \leq A_1 \leq 2^n - 1$, and $A_2 \equiv A_3 + A_4 \times 2^{n-m} - 1$. For another family of generalized Mersenne numbers $N = 2^n - 2^m - 2^{m_1} - 1$, $0 < m_1 < m < \frac{n+1}{2}$, we find that the modular reduction operation $A$ and $N$, where $A < N^2$, can be partially solved as

$$A \mod N \equiv A_1 + A_2 + A_4 + A_6 + 2^m (A_3 + A_4 + A_6) + 2^{m_1} (A_3 + A_4 + A_6 + A_8 \times 2^{n-m}),$$

where $A_1 \equiv A_1 + A_2 \times 2^n$, $0 \leq A_1 \leq 2^n - 1$, $A_2 \equiv A_3 + A_4 \times 2^{n-m}$, $0 \leq A_3 \leq 2^{n-m} - 1$, and $A_4 \equiv A_5 + A_6 \times 2^{m-m_1} - 1$.

Keywords Modular arithmetic, public-key cryptosystems.